10 Ways to Avoid Ethics Dangers in the Cloud

Is Cloud Computing Ethical for Lawyers?

Bob Ambrogi, Esq.
Director of Communications, Catalyst Repository Systems
Is Cloud Computing Ethical for Lawyers?

To date, ethics panels in 17 states have considered that question and every one has answered it “Yes.” But it is a “yes” that comes with a condition. While lawyers may ethically use the cloud, these panels agree, they may do so only if they first take reasonable steps to minimize any risk to confidential client information and client files.

What are the steps a lawyer should take? Each of the ethics panels answered this slightly differently and with greater or lesser degrees of specificity. But they all agree that a lawyer has an obligation to perform a basic level of due diligence about the cloud vendor’s security and reliability.

“[L]awyers may use cloud computing if they take reasonable precautions to ensure that confidentiality of client information is maintained,” The Florida Bar said earlier this year in Opinion 12-3, one typical of other states’ rulings. “The lawyer should research the service provider to be used, should ensure that the service provider maintains adequate security, should ensure that the lawyer has adequate access to the information stored remotely, and should consider backing up the data elsewhere as a precaution.”

To help lawyers research a cloud vendor, here are 10 questions you should ask before putting confidential documents at risk.

1. What is this vendor’s reputation?

With so many Internet start-ups, there is a legitimate fear that a company may be here today but gone tomorrow—and with it your data. Be sure to select a vendor with an established history of operations and growth, strong financial health and a reputation for a quality product with good customer service. Obtain references from other lawyers who have used the service.

2. Will I have unrestricted access to my data?

Several ethics opinions emphasize that, whatever type of cloud service is used, the lawyer must have unfettered access to the data whenever it is needed. One way to ensure this is through a data
escrow agent—an offsite company that maintains encrypted back-ups of the data you host with the vendor. Some cloud providers offer data escrowing as an optional service. Alternatively, you can simply store copies of the data elsewhere so that you will have access to it if the vendor shuts you off.

3. If I stop using the vendor’s service, what happens to my data?

If you discontinue the cloud service, you should have a way to retrieve your data. Ideally, you should be able to retrieve your data in a nonproprietary format (such as a CSV file) that will allow you to import it to another platform. Many cloud services offer their users the ability to download or back up their data.

A more menacing question is that of what happens to the data if the relationship ends on a sour note, such as when the vendor shuts off a customer for nonpayment. Some cloud vendors explicitly promise that customers can continue to have access to download their data, even in the event of a billing dispute.

The flip side of this issue is ensuring that your data is purged from the vendor’s system. Once you terminate your relationship and retrieve your data, you do not want the vendor to maintain back-ups anywhere in its system.

4. Are passwords required to protect access to my data?

Any system worth its salt will have password protection for customer accounts. But many systems take this protection further. Some now offer two-step verification where, after you enter your password, there is a second step to ensure your identity. This may involve sending you a text message with a one-time code you must enter to gain access.

Related to this are features such as automatic log-outs after a certain interval of inactivity. This can prevent unauthorized access to your data when you step away from your computer. The vendor should also be monitoring accounts for suspicious activity that could indicate someone trying to hack into your account.
5. What is the provider’s policy with regard to handling confidential data?

Your agreement with the vendor or its terms of service should expressly address how it and its employees will handle your data in order to protect and preserve confidentiality. Some ethics opinions say that the terms of service (TOS) must expressly include an enforceable obligation to preserve confidentiality and security. In addition, your agreement should require the vendor to give you notice if it is requested to produce your data to a third-party (such as through a subpoena).

6. Does the vendor use encryption?

As data moves from your computer over the Internet to the cloud vendor's servers, it should be encrypted using Secure Socket Lawyers (SSL) encryption of at least 128-bit. SSL not only encrypts your data, but also authenticates to the source to which it is sending. Many vendors now use 256-bit, which is an even higher level of encryption and that much harder to crack.

Your browser will tell you whether you are transmitting data over a secure connection by displaying a padlock icon in the address bar. In Chrome and Opera, the icon displays at the left end of the address bar. In Internet Explorer, Firefox and Safari, it displays at the right end. Also the website’s address will display as “https” instead of “http.”

SSL applies to the transmission of your data. But what happens to it when it arrives on the vendor’s computer servers? Some vendors now offer an additional layer of security by encrypting your data when it is “at rest”—meaning while it is stored on the vendor’s servers. While this can enhance security, it can sometimes limit functionality. Check with the vendor on whether it offers at-rest encryption.

7. What steps will the provider take to back up my data?

Data back-up is a critical issue to ask about with a cloud vendor. Your data should be backed up at least daily. Ideally, your data should be backed up to multiple locations, including locations physically removed from the vendor’s primary storage location.
Even when the vendor has satisfactory back-up measures in place, you should consider making your own back-ups on a regular basis. If your vendor provides a way for you to export or download your data, you should do it on a regular schedule and save it in a secure location.

8. How does the provider protect the security of its data network?

The vendor should be able to provide you with documentation about its standard procedures for protecting network security. It should have firewalls in place and a virus detection program. In addition, it should be running regular scans of its systems and its ports by which it monitors unauthorized intrusions, network usage and application usage.

9. How does the provider protect the physical security of its data center?

It is important to know the physical location and security measures in place at the vendor’s data center. To protect the physical integrity of its systems, the vendor’s data center should have:

- 24x7 on-site security, including video monitoring and access verification.
- Uninterruptible, redundant power supplies, including on-site generators.
- Redundant cooling systems to keep the internal climate at the optimum temperature and humidity.
- Fire detection and suppression, including off-site alarm monitoring and dispatch.
- System monitoring, with 24x7, real-time monitoring of all essential systems.

Few cloud vendors have their own data centers. Most use a third-party colocation facility, where the vendor can house its own hardware and software, or an establish cloud infrastructure such as Amazon Web Services.

Several ethics opinions emphasize that the lawyer must have unfettered access to the data whenever it is needed.
A shortcut to evaluating a vendor’s security is to look for whether it is SSAE 16 or SAS 70 certified. This is an auditing standard developed by the American Institute of Certified Public Accountants to verify that controls are in place to protect financial information. It can apply to data centers, colocation facilities, cloud providers and other companies that deal with sensitive data.

10. What are the vendor’s terms of service?

Maybe the most important step you can take is to carefully review the vendor’s terms of service (TOS) and any licensing agreements or other service agreements. Look for any red flags in these documents and for any explicit provisions pertaining to confidentiality, security and data ownership.

Unfortunately, there is no 100 percent foolproof way to secure your data ever, whether you store it in the cloud or locally. However, by asking these 10 questions of a cloud vendor, you can be reasonably assured that your clients’ information will remain safe and secure.

About the Author

Bob Ambrogi is a lawyer and veteran legal journalist, and advises Catalyst on strategic communications and marketing matters. He is also a practicing lawyer in Massachusetts and is the former editor-in-chief of The National Law Journal, Lawyers USA and Massachusetts Lawyers Weekly. A fellow of the College of Law Practice Management, he also writes the blog LawSites.